대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0024173
Application Number

출 원 년 월 일 : 2003년 04월 16일
Date of Application APR 16, 2003

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2004 년 02 월 20 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0005
【제출일자】	2003.04.16
【발명의 명칭】	개별적으로 존재하는 네트워크를 연결하는 장치 및 방법
【발명의 영문명칭】	DEVICE AND METHOD OF CONNECTING NETWORK BEING SEPARATELY
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	김동진
【대리인코드】	9-1999-000041-4
【포괄위임등록번호】	2002-007585-8
【발명자】	
【성명의 국문표기】	육현규
【성명의 영문표기】	YOOK,Hyun Gyoo
【주민등록번호】	700623-1231719
【우편번호】	152-082
【주소】	서울특별시 구로구 고척2동 251-31
【국적】	KR
【발명자】	
【성명의 국문표기】	윤현식
【성명의 영문표기】	YOON,Hyun Sik
【주민등록번호】	730126-1012210
【우편번호】	134-090
【주소】	서울특별시 강동구 상일동 우성빌라 6동 303호
【국적】	KR
【발명자】	
【성명의 국문표기】	김도헌
【성명의 영문표기】	KIM,Do Heon
【주민등록번호】	700619-1351212

【우편번호】	135-010
【주소】	서울특별시 강남구 논현동 10-3 303호
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 김동진 (인)
【수수료】	
【기본출원료】	20 면 29,000 원
【가산출원료】	15 면 15,000 원
【우선권주장료】	0 건 0 원
【심사청구료】	26 항 941,000 원
【합계】	985,000 원
【첨부서류】	1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 제1 네트워크에서 전송된 네트워크간 연결요청 메세지를 수신하여 상기 자신의 네트워크와 상기 제1 네트워크를 연결시키고, 상기 연결된 제1 네트워크에 대한 시큐리티 레벨을 설정하며, 상기 설정된 레벨에 따라 네트워크 명령 메세지를 제어하는 결합 모듈을 포함하는 것을 특징으로 하며, 개별적으로 존재하는 네트워크들을 상호 연결 시킴으로써 동일한 네트워크에 존재하지 않는 디바이스를 상호 연결하여 제어할 수 있는 잇점이 있다.

【대표도】

도 3

【색인어】

네트워크 연결 장치, 결합 모듈, 게이트웨이

【명세서】

【발명의 명칭】

개별적으로 존재하는 네트워크를 연결하는 장치 및 방법{DEVICE AND METHOD OF CONNECTING NETWORK BEING SEPARATELY}

【도면의 간단한 설명】

도 1은 종래의 홈 네트워크 망을 개략적으로 나타낸 도면.

도 2는 종래의 홈 네트워크에 존재하는 UPnP 제어 디바이스를 제어하기 위한 동작 과정을 나타낸 도면으로서, 2a는 디스커버리 과정을 나타낸 도면이고, 2b 디스크립션 과정을 나타낸 도면이고, 2c는 제어 동작 과정을 나타낸 도면이고, 2d는 이벤트 과정을 나타낸 도면이다.

도 3은 본 발명에 따른 개별적으로 존재하는 네트워크를 연결하는 장치가 서로 연결되어 있는 구성을 개략적으로 나타낸 도면.

도 4는 본 발명에 따른 개별적으로 존재하는 네트워크를 연결하는 장치의 내부 구성도.

도 5는 본 발명에 따른 개별적으로 존재하는 네트워크를 연결하는 장치 중 결합 모듈의 내부 구성도.

도 6은 본 발명에 따른 개별적으로 존재하는 네트워크를 연결하는 장치 중 결합 모듈의 내부 동작을 나타낸 도면.

도 7은 본 발명에 따른 개별적으로 존재하는 네트워크를 연결하는 방법을 개략적으로 나타낸 흐름도.

< 도면의 주요부분에 대한 부호의 설명 >

100 : 네트워크 연결 장치 110 : 스택 모듈

120 : 관리 모듈 130 : 컴포넌트 모듈

140 : 룩 업 서비스 모듈 150 : 결합 모듈

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<12> 본 발명은 개별적으로 존재하는 네트워크를 연결하는 장치 및 방법에 관한 것으로서, 개별적으로 구성된 네트워크들을 연결시켜 각 네트워크 상에 존재하는 디바이스들을 상호 제어할 수 있도록 하는 개별적으로 존재하는 네트워크를 연결하는 장치 및 방법에 관한 것이다.

<13> 일반적으로, 홈 네트워크는 인터넷 프로토콜(Internet Protocol : 이하 IP라 함) 기반의 사설 망(Private network)으로 이루어지는 것으로, 가정 내에서 사용되는 모든 형태의 개인 컴퓨터(PC)와 지능형 제품, 무선 장치 등의 다양한 기기들을 하나의 네트워크로 연결하여 통제하는 것이다.

<14> 도 1은 종래의 홈 네트워크 망을 개략적으로 나타낸 도면으로서, UPnP 홈 네트워크의 구성은 크게 제어를 받는 UPnP 제어 디바이스(UPnP Controlled Device : 이하 UPnP CD라 함)(20)와 상기 UPnP CD(20)를 제어하기 위한 UPnP 제어 포인트(UPnP Control Point : 이하 UPnP CP라 함)(10)로 나뉘어진다.

<15> 상기 UPnP CD(20)는 여러 UPnP 디바이스들을 포함할 수 있으며, 각 디바이스는 자신의 기능에 따라 특정 서비스를 구현하고, 상기 UPnP CP(10)는 특정 디바이스의 서비스를 설명해 놓은 XML파일을 분석하여 UPnP CD(20)를 제어한다.

<16> 도 2는 종래의 홈 네트워크에 존재하는 UPnP 제어 디바이스를 제어하기 위한 동작 과정을 나타낸 것으로, 현재 UPnP 홈 네트워크에서의 UPnP 디바이스를 제어하기 위해서는 디스커버리 과정과 디스크립션(Description) 과정을 수행하여 UPnP CD(20)의 정보를 얻을 수 있고, 상기 과정 통해 얻어진 홈 네트워크에 연결된 UPnP CD(20)의 정보를 통해 UPnP CD(20)를 제어할 수 있다. 여기서, 상기 디스커버리 과정을 통해 UPnP CP(10)가 제어 하고자 하는 디바이스를 찾고, 상기 디스크립션 과정을 통해서 상기 디스커버리 과정에서 찾은 UPnP 디바이스의 서비스 템플릿(Service Template) XML을 읽음으로써 UPnP CP(10)가 특정 디바이스에 어떤 명령을 내릴 수 있는가를 분석하며, 제어 과정을 통해서 UPnP CP(10)가 제어하고자 하는 UPnP 디바이스의 특정 서비스에 SOAP 메시지 형태로 명령을 보내어 UPnP 디바이스를 제어하는 것이다. 한편, UPnP CD(20)는 변경된 자신의 정보를 UPnP CP(10)로 전송하는 이벤트(Event) 과정을 수행한다.

<17> 도 2a는 디스커버리 과정을 나타낸 도면으로서, 디스커버리 과정은 크게 두 가지로 나누어 설명할 수 있다. 하나는 새로운 UPnP 디바이스가 홈 네트워크 내에 들어오게 되는 경우이고, 다른 하나는 UPnP CP(10)가 홈 네트워크에 들어오게 되는 경우이다.

<18> 먼저, UPnP 디바이스(예를 들어, UPnP CD 1)가 네트워크상에 들어오게 되는 경우를 어드버타이징(Advertising)이라 하며, 이 경우는 UPnP 디바이스가 멀티캐스트(multicast) 메세지를 보내어 UPnP CP(10)에게 자신의 존재를 알려 준다. 즉, UPnP CP(10)가 존재하는 상태에서 UPnP 디바이스가 네트워크 상에 들어오고, 그 다음 어드레싱(Addressing) 과정을 통해 자신의 고유 URL을 배정받은 후 자신의 존재를 멀티캐스트 메세지로 네트워크 상의 모든 디바이스 또는 UPnP CP(10)에게 보낸다. 상기 UPnP 디바이스를 제어하기 원하는 UPnP CP(10)는 상기 UPnP 디바이스가 멀티캐스트한 메세지를 받아 등록한다.

<19> 반대로, UPnP 디바이스들이 네트워크상에 존재하고 있는 상태에서 UPnP CP(10)가 새로이 홈 네트워크상에 들어오게 되는 경우는, 상기 UPnP CP(10)가 멀티캐스트 메세지를 보내면, UPnP 디바이스는 자신을 찾고 있는 UPnP CP(10)에게 유니캐스트(unicast) 메세지를 전송한다. 즉, UPnP 디바이스가 어드레싱 과정을 끝내고 자신의 URL을 배정받은 상태에서 UPnP CP(10)가 멀티캐스트한 서치 메세지를 받아 자신을 찾고 있는 UPnP CP(10)에게 유니캐스트 응답(response) 메세지를 보내면, 상기 응답 메세지를 받은 UPnP CP(10)는 상기 UPnP 디바이스를 등록한다.

<20> 도 2b는 디스크립션 과정을 나타낸 것으로,. 디스크립션 과정은 UPnP CP(10)가 UPnP 디바이스를 제어하기 위해 필요한 서비스 기능들을 상기 UPnP 디바이스가 제공하는 서비스. 디스크립션(Descripton) XML 파일을 분석하여 얻게 되는 과정을 말한다. 즉, UPnP 디바이스를 제어하고자 하는 UPnP CP(10)가 상기 UPnP 디바이스에게 디스크립션 XML 파일을 요청하고 상기 요청된 디스크립션 XML 파일을 파싱(Parsing)한다.

<21> 도 2c는 제어 과정을 나타낸 것으로, 제어 과정은 UPnP 디바이스가 어드레싱 과정과 디스커버리 과정을 통해서 UPnP 디바이스와 UPnP CP(10)가 서로의 URL 어드레스를 알고 있는 상태에서 UPnP CP(10)가 제어 하고자 하는 UPnP 디바이스의 특정 서비스에 SOAP 메시지 형태로 명령을 보내는 것을 말한다. 즉, UPnP CP(10)가 제어하기 원하는 UPnP 디바이스에 대한 서비스 템플릿을 전송함으로써 UPnP 디바이스를 직접 제어 할 수 있다.

<22> 도 2d는 이벤트 과정을 나타낸 것으로, 이벤트 과정은 UPnP CP(10)가 원하는 UPnP CD(20)의 정보 변경 상태 알고자 할 경우 해당 UPnP CD(10)에 서브스크라이브(subscribe)을 요청하면, 해당 UPnP CD(20)는 상기 서브스크라이브를 요청한 UPnP CP(10)에게 자신의 정보가 변경될 때마다 자신의 변경된 정보를 알려주는 이벤팅 메시지를 전송하는 것을 말한다.

<23> 그러나, 종래의 홈 네트워크 기술은 가정 내에서만 가능하기 때문에 공간적인 제약이 있었다. 즉, 가정 내의 디바이스 연결은 로컬로 구성되어, UPnP는 하나의 홈 네트워크 망에서만 동작한다. 따라서, UPnP 자체로는 두 개 이상의 개별적인 홈 네트워크를 유동적으로 연결할 수 없는 문제점이 있다.

【발명이 이루고자 하는 기술적 과제】

<24> 본 발명은 상기한 문제점을 해결하기 위하여 안출된 것으로서, 본 발명의 목적은 개별적으로 구성된 네트워크들을 연결시켜 각 네트워크 상에 존재하는 디바이스들을 상호 제어할 수 있도록 하는 개별적으로 존재하는 네트워크를 연결하는 장치 및 방법을 제공하는 것이다.

【발명의 구성 및 작용】

<25> 상기 목적을 달성하기 위하여 본 발명은, 제1 네트워크에서 전송된 네트워크간 연결요청 메세지를 수신하여 상기 자신의 네트워크와 상기 제1 네트워크를 연결시키고, 상기 연결된 제1 네트워크에 대한 시큐리티 레벨을 설정하며, 상기 설정된 레벨에 따라 네트워크 명령 메세지를 제어하는 결합 모듈을 포함하는 것을 특징으로 한다.

<26> 또한, 제1 네트워크가 제2 네트워크로 초기 네트워크간 연결요청 메세지를 전송하는 단계와, 상기 제2 네트워크가 상기 전송된 초기 네트워크간 연결요청 메세지를 분석하여 상기 제1 네트워크에 대한 시큐리티 레벨을 설정하는 단계와, 상기 제1 네트워크가 제2 네트워크로 네트워크 명령 메세지를 전송하는 단계와, 상기 제2 네트워크가 상기 네트워크 명령 메세지를 전송한 제1 네트워크의 상기 설정된 시큐리티 레벨을 검색하는 단계 및 상기 검색된 시큐리티 레벨 및 전송된 네트워크 명령 메세지를 제2 네트워크로 전송하는 단계를 포함하는 것을 특징으로 한다.

<27> 이하, 첨부한 도면들을 참조로 본 발명의 바람직한 실시예를 상세히 설명한다.

<28> 도 3은 본 발명에 따른 개별적으로 존재하는 네트워크를 연결되어 있는 구성을 개략적으로 나타낸 도면으로서, 네트워크를 외부와 연결시키는 게이트웨이 내에 네트워크 연결 장치(100)가 구비된 구성이다. 즉, 개별적으로 존재하는 네트워크들을 네트워크 연결 장치(100)를 통해 상호 연결시킴으로써, 동일한 네트워크 상에 존재하지 않는 디바이스(200)들도 상호 제어할 수 있다.

<29> 도 4는 본 발명에 따른 개별적으로 존재하는 네트워크를 연결하는 장치의 내부 구성도로서, 네트워크 연결 장치(100)는 스택 모듈(110), 관리 모듈(120), 컴포넌트 모듈(130), 룩 업 서비스 모듈(140) 및 결합 모듈(150)로 구성된다.

<30> 네트워크 연결 장치(100)는 네트워크의 상에 존재하는 디바이스(200)들의 정보를 관리하고, 각 네트워크 상에 존재하는 디바이스(200)들을 상호 연결시킴으로써 동일한 네트워크 상에 존재하는 디바이스(200)가 아니더라도 원하는 디바이스들을 제어할 수 있도록 한다.

<31> 관리 모듈(120)은 네트워크 상에 존재하는 디바이스(200)들에게 디스커버리 과정을 수행하여 각 디바이스(200)들의 정보를 수집 관리 한다. 즉, 네트워크 상에 존재하는 디바이스(200)들에 서치 메세지를 보내고, 상기 디바이스(200)로부터 전송받은 응답 메세지를 수신하여 네트워크 상에 존재하는 디바이스(200)를 찾고, 상기 발견된 디바이스의 디스크립션(Description)을 요청하여 디바이스의 정보를 얻을 수 있다. 또한, 상기 관리 모듈(120)은 주기적으로 네트워크 상에 존재하는 디바이스(200)들을 체크한다.

<32> 컴포넌트 모듈(130)은 상기 관리 모듈(120)에서 수집한 디바이스(200)들의 정보를 기초로 하여 네트워크 상에 존재하는 디바이스(200)들의 서비스를 나타내는 컴포넌트를 생성한다.

여기서, 상기 컴포넌트는 네트워크 상에 존재하는 디바이스(200)에 대한 명령, 동작 및 각 동작에 대한 서비스 응답 등을 포함한다.

<33> 룩 업 서비스 모듈(140)은 상기 컴포넌트 모듈(130)이 생성한 컴포넌트의 정보를 룩 업(Lookup) 테이블에 저장하고, 특정 디바이스의 서비스 요청시 해당 디바이스의 컴포넌트 정보를 검색한다. 여기서, 상기 룩 업 서비스 모듈(140)은 컴포넌트 정보를 룩 업 테이블로 저장하기 때문에 편리하게 해당 컴포넌트 정보를 검색할 수 있다.

<34> 결합 모듈(150)은 제1 네트워크에서 전송된 네트워크간 연결요청 메세지를 수신하여 상기 자신의 네트워크와 상기 제1 네트워크를 연결시키고, 상기 연결된 제1 네트워크에 대한 시큐리티 레벨을 설정하며, 상기 설정된 레벨에 따라 네트워크 명령 메세지를 제어한다. 상기 결합 모듈은 하기 도 5에서 더 자세히 설명한다.

<35> 스택 모듈(110)은 상기 네트워크 상에 존재하는 디바이스(200)들에게 제어 메세지를 전송하는 것이다.

<36> 도 5는 본 발명에 따른 개별적으로 존재하는 네트워크를 연결하는 장치 중 결합 모듈의 내부 구성도로서, 결합 모듈(150)은 연결(connection) 모듈(151), 인증/시큐리티(authentication/security) 모듈(152) 및 전송(transit) 모듈(153)로 구성된다.

<37> 연결 모듈(151)은 제1 네트워크가 전송하는 네트워크간 연결요청 메세지 수신 및 각 네트워크들을 상호 연결시켜 준다. 여기서, 상기 연결 모듈(151)은 상기 네트워크간 연결요청 메세지를 전송한 제1 네트워크 및 상기 제1 네트워크상에 존재하는 디바이스의 연결 정보(예를 들어, 공개(public) IP 주소 및 포트 번호 등)를 가지고 있다. 즉, 연결 모듈(151)은 연결을 요청한 디바이스(200)의 공개 IP 주소 또는 디바이스(200)가 속한 네트워크의 게이트웨이의 공

개 IP 주소를 관리하고, 상기 연결 모듈(152)에서 메시지 전송시 해당 디바이스(200)의 IP 주소 또는 디바이스(200)가 속한 네트워크의 게이트웨이의 공개 IP 주소를 통해 메시지를 보낼 수 있으며, 여기서 상기 공개 IP 주소로 보내는 메시지 타입은 Http Post 형태로 이해될 수 있다.

<38> 또한, 상기 연결 모듈(151)은 일정 시간 마다 네트워크간 연결요청 메세지를 전송한 제1 네트워크가 네트워크 명령 메세지를 전송하는지 체크하여 상기 제1 네트워크로부터 일정 시간 내에 네트워크 명령 메세지가 수신되지 않으면 상호 연결된 디바이스의 연결을 해지시킨다. 또한, 상기 네트워크간 연결요청 메세지를 전송한 제1 네트워크가 상기 제2 네트워크에게 해지를 알리는 메시지를 보내어 자신을 연결 리스트(connection list)에서 제거하게 한 후 자신의 연결 리스트에서도 해당 디바이스를 제거하여 연결을 해지시킨다.

<39> 인증 모듈(152)은 상기 연결 모듈(151)에 네트워크간 연결요청 메세지를 전송한 제1 네트워크에 대한 연결허용 여부와 시큐리티 레벨(security level)을 설정 및 체크한다. 또한, 상기 인증 모듈(152)은 상기 네트워크간 연결요청 메세지를 전송한 제1 네트워크에 대한 네트워크의 연결허용 결정 및 그에 따른 시큐리티 레벨 정보를 저장/보관한다. 여기서, 상기 연결허용 여부는 네트워크간 연결요청 메세지를 전송한 제1 네트워크의 연결 정보를 확인하여, 연결하고 싶지 않은 제1 네트워크인 경우 연결을 거부하고, 연결을 원하는 제1 네트워크인 경우에만 연결을 허용 시킨다. 그리고, 상기 시큐리티 레벨은 네트워크간 연결요청 메세지를 전송한 제1 네트워크에 따라 다르게 적용된다. 즉, 자신의 네트워크 상에 존재하는 디바이스에 각각 레벨을 설정해 놓은 상태에서 네트워크간 연결요청 메세지를 전송한 제1 네트워크가 연결 되면, 상기 설정해 놓은 레벨을 기준으로 상기 제1 네트워크에 연결시

킬 디바이스와 연결 시키지 않을 디바이스를 결정한다. 따라서, 중요한 디바이스인 경우 레벨을 높게 설정하여 제1 네트워크에 연결 시킬때 레벨이 낮게 설정된 디바이스들만이 보여지게 한다.

<40> 전송 모듈(153)은 상기 인증/시큐리티 모듈(152)이 연결을 허용한 제1 네트워크가 요청한 네트워크 명령 메세지를 전송한다. 여기서 상기 네트워크 명령 메세지는 상기 제1 네트워크와 제2 네트워크 사이에 송수신 되는 모든 메세지를 말하며, 예를 들어 디스커버리 메세지, 통지(notify) 메세지, 컨트롤 메세지 및 디바이스 정보 요청 메세지 등으로 이해될 수 있다. 또한, 상기 전송 모듈(153)은 제1 네트워크에서 특정 디바이스 정보를 요청하면, 연동된 룩 업 서비스 모듈(140) 내의 룩 업 테이블에 저장된 특정 디바이스의 정보를 전송한다.

<41> 도 6은 본 발명에 따른 개별적으로 존재하는 네트워크를 연결하는 장치 중 결합 모듈의 내부 동작을 나타낸 도면이다.

<42> 도 6a는 제1 네트워크가 제2 네트워크로 초기 네트워크간 연결 메세지 전송 및 그에 따른 시큐리티 레벨을 설정하는 과정을 나타낸 도면으로서, 먼저 상기 제1 네트워크가 제2 네트워크로 초기 네트워크간 연결 메세지를 전송하면, 상기 연결 모듈(151)은 상기 전송된 초기 네트워크간 연결 메세지를 인증/시큐리티 모듈(152)로 전송한다.

<43> 그 다음, 상기 인증/시큐리티 모듈(152)은 상기 전송받은 초기 네트워크간 연결 메세지를 분석하여 상기 제1 네트워크에 대한 시큐리티 레벨을 설정 및 저장한다. 여기서, 상기 시큐리티 레벨은 상기 연결되는 제1 네트워크에 따라 다르게 적용된다.

<44> 도 6b는 제2 네트워크가 제1 네트워크로부터 네트워크 명령 메세지를 전송받는 경우를 나타낸 도면으로서, 제1 네트워크로부터 네트워크 명령 메세지가 전송되면 연결 모듈(151)이

상기 전송된 네트워크 명령 메세지를 수신하고, 전송 모듈(153)에 상기 전송된 네트워크 명령 메세지를 보낸다. 그러면, 상기 전송 모듈(153)은 보안/시큐리티 모듈(152)에게 상기 제1 네트워크로부터 전송받은 네트워크 명령 메세지에 대한 시큐리티 레벨을 검색하고, 상기 검색된 시큐리티 레벨과 네트워크 명령 메세지를 제2 네트워크로 전송하다.

<45> 도 6c는 제2 네트워크가 제1 네트워크가 요청한 네트워크 명령 메세지에 따른 응답 메세지를 전송하는 경우를 나타낸 도면으로서, 먼저 제2 네트워크가 전송 모듈(153)를 통해 제1 네트워크로 전송할 응답 메세지를 보내면, 상기 보안/시큐리티 모듈(152)이 상기 제2 네트워크가 전송한 응답 메세지에 대한 시큐리티 레벨을 체크하여 전송 가능한 응답 메세지인가를 체크한다. 상기 체크 결과 전송 가능한 응답 메세지인 경우, 전송 모듈(153)은 해당 응답 메세지를 연결 모듈(151)로 전송하고, 이에 상기 연결 모듈(151)은 제1 네트워크로 상기 응답 메세지를 전송한다.

<46> 도 7은 본 발명에 따른 개별적으로 존재하는 네트워크를 연결하는 방법을 개략적으로 나타낸 흐름도로서, 먼저 제1 네트워크가 제2 네트워크로 초기 네트워크간 연결요청 메세지를 전송하면(S100), 상기 제2 네트워크의 연결 모듈(151)은 상기 전송된 초기 네트워크간 연결요청 메세지를 전송 모듈(153)로 보낸다. 여기서, 상기 초기 네트워크간 연결요청 메세지에는 제1 네트워크에 대한 정보를 포함하고 있다.

<47> 이에, 상기 전송 모듈(153)은 전송받은 초기 네트워크간 연결요청 메세지를 보안/시큐리티 모듈(152)로 전송하여 상기 제1 네트워크의 연결 허용 여부 및 시큐리티 레벨을 설정하도록 한다(S102). 여기서, 상기 시큐리티 레벨 설정은 상기 연결되는 제1 네트워크에 따라 다르게 적용되며, 상기 설정된 시큐리티 레벨은 네트워크 별로 보안/시큐리티 모듈(152)에 저장된다.

<48> 그 다음, 상기 제1 네트워크에 대해 연결허용이 되면, 상기 제1 네트워크가 상기 제2 네트워크로 네트워크 명령 메세지를 전송하고, 상기 네트워크 명령 메세지를 전송한 제1 네트워크의 상기 설정된 시큐리티 레벨을 검색한다(S104 내지 S108).

<49> 이 후, 상기 검색된 제1 네트워크의 시큐리티 레벨과 네트워크 명령 메세지를 제2 네트워크로 전송한다(S110). 여기서, 상기 제2 네트워크가 상기 제1 네트워크로부터 전송받은 네트워크 명령 메세지에 대한 응답 메세지를 전송할 경우, 보안/시큐리티 모듈(152)은 상기 전송될 응답 메세지에 대한 시큐리티 레벨을 체크하여, 시큐리티 레벨에 적합한 응답 메세지가 전송되는 지를 체크한다. 여기서, 상기 시큐리티 레벨에 적합한 응답 메세지 인가를 확인하는 것은 상기 설정되어 있는 시큐리티 레벨보다 높은 레벨, 즉 제1 네트워크에 전송하지 않아야 하는 레벨의 디바이스가 전송되는지를 확인하기 위해서이다.

<50> 상기 제1 네트워크의 시큐리티 레벨과 네트워크 명령 메세지를 제2 네트워크로 전송되면, 상기 제2 네트워크는 상기 제1 네트워크로 통지 메세지를 전송하여 상기 제2 네트워크에 연결되어 있는 디바이스들을 알려준다(S112). 여기서, 상기 제2 네트워크는 상기 제1 네트워크의 시큐리티 레벨에 해당하는 디바이스들만을 선별하여 제1 네트워크에 전송한다.

<51> 한편, 상기 제1 네트워크가 전송한 네트워크 명령 메세지가 제2 네트워크 내 디바이스를 찾는 서치 메세지인 경우, 상기 제2 네트워크는 상기 검색된 제1 네트워크의 시큐리티 레벨에 해당하는 디바이스들을 검색하여 상기 제1 네트워크로 전송해 주며(S118,S120), 상기 제1 네트워크가 전송한 네트워크 명령 메세지가 제2 네트워크 내 특정 디바이스를 요청하는 메세지인 경우, 상기 제2 네트워크는 상기 룩 업 서비스 모듈(140)에 저장된 해당 디바이스의 컴포넌트를 검색하여 상기 제1 네트워크로 전송해 준다.

<52> 이에, 상기 제1 네트워크는 제어를 원하는 디바이스를 제2 네트워크의 디바이스 정보를 요청하면, 상기 제2 네트워크는 해당 디바이스에 대한 컴포넌트를 검색하여 제1 네트워크로 전송한다(S114,S116). 따라서, 상기 제1 네트워크는 상기 제2 네트워크 상에 연결된 디바이스를 제어할 수 있다. 즉, 상기 제1 네트워크와 제2 네트워크는 동일한 네트워크 상이 아니더라도 원하는 디바이스를 제어할 수 있다.

<53> 한편, 제1 네트워크가 제2 네트워크에게 현재 연결된 디바이스의 연결해지 요청 메세지를 전송하면, 상기 제2 네트워크는 자신의 디바이스와 연결되어 있는 제1 네트워크를 연결 리스트(connection list)에서 삭제하고, 상기 제2 네트워크도 현재 연결된 제2 네트워크 상에 존재하는 디바이스를 연결 리스트에서 삭제한다. 또한, 상기 제1 네트워크에서 일정 시간 동안 네트워크 명령 메세지가 수신되지 않으면, 제2 네트워크는 자동으로 제1 네트워크와의 연결을 해지한다.

<54> 본 발명에 따른 바람직한 실시예를 설명하면, 우리 집의 CD 플레이어에 있는 노래를 친구가 자신의 집에서 듣고자 한다. 여기서, 상기 CD 플레이어는 UPnP AV MediaServer의 기능을 가지고 있는 UPnP 디바이스이고, 외부로 연결된 게이트웨이 상의 네트워크 연결 장치(100)에 등록이 되어 있는 상태이다.

<55> 먼저, 내가 친구에게 내 게이트웨이의 공개 IP 주소와 네트워크 연결 장치(100)로 연결되는 포트 번호를 알려주어 친구가 내 네트워크에 네트워크간 연결요청을 할 수 있도록 한다. 여기서, 내 게이트웨이가 자체 웹 서버를 가지고 있어 친구에게 웹 주소를 알려주고, 웹 페이지에 연결하게 한 후 연결 요청 버튼을 누르게 하여 연결을 요청할 수도 있다.

<56> 그 다음, 상기 친구가 네트워크가 연결요청 메세지를 전송하면 연결 포트(151)를 통해 상기 네트워크간 연결요청 메세지가 전달되며, 상기 네트워크간 연결요청 메세지는 게이트웨이에 연결된 또는 네트워크 연결 장치(100)에 연결된 모니터를 통해서 보여진다.

<57> 이에, 상기 전송된 네트워크간 연결요청 메세지가 친구가 보낸 네트워크간 연결요청 메세지인가를 확인한 후, 친구의 네트워크 연결을 허락하고 상기 친구의 네트워크에 대한 시큐리티 레벨을 설정한다. 예를 들어, 친구의 네트워크에 대한 시큐리티 레벨을 2로 맞춰 놓으면, 이 후 친구가 내 네트워크에 연결시 내 네트워크 상에 존재하는 디바이스들 중 레벨 2에 해당하는 디바이스들만을 연결된다. 즉, 상기 CD 플레이어의 현재 시큐리티 레벨은 2로 맞추어져 있는 상태이고, 레벨이 2 및 1로 맞추어져 있는 디바이스들은 상기 친구에게 제공된다. 만약, 친구에게 연결시키지 않을 디바이스가 존재할 경우, 그 디바이스의 레벨을 2 이상으로 설정하면, 상기 디바이스는 친구의 네트워크로 연결되지 않는다. 한편, 상기 친구의 연결을 허락하고 보안 레벨을 2로 설정한 정보는 보안 모듈(152)에 저장된다.

<58> 그 다음, 친구가 연결되면 전송 모듈(153)은 시큐리티 레벨이 2 이하인 다바이스들의 통지 메세지를 연결 모듈(151)을 통해 친구의 네트워크로 전송한다.

<59> 이에, 친구는 상기 전송된 통지 메세지를 분석하여 원하는 디바이스의 정보(여기서는 CD 플레이어의 서비스 정보)를 요청한다. 이로써, 상기 친구는 우리 집 거실에 있는 CD 플레이어를 찾을 수 있게 되고, 상기 친구는 자신의 집에 있는 UPnP MediaRenderer기능을 가지고 있는 CD 플레이어를 통해 원하는 음악들을 수 있다.

<60> 한편, 상기 친구가 원하는 CD를 다 듣고 난 후 연결 해지를 요청하면, 상기 연결 해지 요청 메세지가 연결 모듈(151)을 통해 내 네트워크로 전송된다. 여기서, 내가 친구가 CD를 다 들었는지 물어보고 해지를 할 수도 있다. 즉, 연결 해지 요청을 하게 되면 연결 모듈(151)은

전송 모듈(153)에게 해지를 요청하는 메시지를 보내고 자신의 연결 리스트에서 해당 디바이스의 연결 정보를 삭제한다. 또한 인증/시큐리티 모듈(152)에 요청하여 해당 디바이스의 정보를 지우거나 더 이상 관리하지 않도록 하며, 전송 모듈(153)은 네트워크의 메세지가 연결 모듈(151)을 통해 외부로 나가지 않도록 한다.

<61> 이상에서 본 발명에 대하여 상세히 기술하였지만, 본 발명이 속하는 기술 분야에 있어서 통상의 지식을 가진 사람이라면, 첨부된 청구범위에 정의된 본 발명의 정신 및 범위를 벗어나지 않으면서 본 발명을 여러 가지로 변형 또는 변경하여 실시할 수 있음은 자명하며, 따라서 본 발명의 실시예에 따른 단순한 변경은 본 발명의 기술을 벗어날 수 없을 것이다.

【발명의 효과】

<62> 상기한 구성의 본 발명에 의하면, 개별적으로 존재하는 네트워크들을 상호 연결 시킴으로써 동일한 네트워크에 존재하지 않는 디바이스도 상호 연결하여 제어할 수 있는 잇점이 있다.

<63> 또한, 사용자가 연결을 요청하는 네트워크에 대해 연결허용 여부 및 시큐리티 레벨을 임의로 설정할 수 있어 원하지 않는 네트워크의 연결을 피할 수 있는 잇점이 있다.

【특허청구범위】

【청구항 1】

제1 네트워크에서 전송된 네트워크간 연결요청 메세지를 수신하여 상기 자신의 네트워크와 상기 제1 네트워크를 연결시키고, 상기 연결된 제1 네트워크에 대한 시큐리티 레벨을 설정하며, 상기 설정된 레벨에 따라 네트워크 명령 메세지를 제어하는 결합 모듈을 포함하는 것을 특징으로 하는 네트워크 연결 장치.

【청구항 2】

제 1항에 있어서, 상기 결합 모듈은,

제 1 네트워크가 전송하는 네트워크간 연결요청 메세지 수신 및 각 네트워크들을 상호 연결시켜 주는 연결 모듈;

상기 연결 모듈에 네트워크간 연결요청 메세지를 전송한 제1 네트워크에 대한 연결허용 여부와 시큐리티 레벨을 설정 및 체크하는 인증/시큐리티 모듈; 및

상기 인증/시큐리티 모듈이 연결을 허용한 제1 네트워크가 요청한 네트워크 명령 메세지를 전송하는 전송 모듈을 포함하는 것을 특징으로 하는 네트워크 연결 장치.

【청구항 3】

제 1항에 있어서,

네트워크 상에 존재하는 디바이스들에게 디스커버리 과정을 수행하여 각 디바이스들의 정보를 수집 관리하는 관리 모듈;

상기 관리 모듈에서 수집한 디바이스들의 정보를 기초로 하여 네트워크 상에 존재하는 디바이스들의 서비스를 나타내는 컴포넌트를 생성하는 컴포넌트 모듈을 포함하는 것을 특징으로 하는 네트워크 연결 장치.

【청구항 4】

제 1항에 있어서,

상기 네트워크 상에 존재하는 디바이스들에게 제어 메세지를 전송하는 스택 모듈; 및

상기 컴포넌트 모듈이 생성한 컴포넌트의 정보를 룩 업 테이블에 저장하고, 특정 디바이스의 서비스 요청시 해당 디바이스의 컴포넌트 정보를 검색하는 룩 업 서비스 모듈을 더 포함하는 것을 특징으로 하는 네트워크 연결 장치.

【청구항 5】

제 2항에 있어서, 상기 연결 모듈은,

네트워크 또는 네트워크 상에 존재하는 디바이스의 연결 정보를 가지고 있는 것을 특징으로 하는 네트워크 연결 장치.

【청구항 6】

제 2항에 있어서, 상기 연결 모듈은,

제1 네트워크에서 일정 시간 마다 네트워크 명령 메세지를 전송하는지를 체크하여 일정 시간 내에 네트워크 명령 메세지가 수신되지 않으면 상호 연결된 네트워크들의 연결을 해지하는 것을 특징으로 하는 네트워크 연결 장치.

【청구항 7】

제 2항에 있어서, 시큐리티 레벨은,

상기 연결되는 제1 네트워크에 따라 다르게 적용되는 것을 특징으로 하는 네트워크 연결 장치.

【청구항 8】

제 2항에 있어서, 상기 전송 모듈은,

상기 자신의 네트워크와 제1 네트워크 사이에 송수신 되는 네트워크 명령 메세지를 전송하는 것을 특징으로 하는 네트워크 연결 장치.

【청구항 9】

제1 네트워크가 제2 네트워크로 초기 네트워크간 연결요청 메세지를 전송하는 단계;

상기 제2 네트워크가 상기 전송된 초기 네트워크간 연결요청 메세지를 분석하여 상기 제1 네트워크에 대한 시큐리티 레벨을 설정하는 단계;

상기 제1 네트워크가 제2 네트워크로 네트워크 명령 메세지를 전송하는 단계;

상기 제2 네트워크가 상기 네트워크 명령 메세지를 전송한 제1 네트워크의 상기 설정된 시큐리티 레벨을 검색하는 단계; 및

상기 검색된 시큐리티 레벨 및 전송된 네트워크 명령 메세지를 제2 네트워크로 전송하는 단계를 포함하는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【청구항 10】

제 9항에 있어서, 상기 네트워크간 연결요청 메세지는,

상기 네트워크간 연결요청 메세지를 보낸 제1 네트워크에 대한 정보를 포함하는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【청구항 11】

제 9항에 있어서, 상기 시큐리티 레벨은,

상기 연결되는 제1 네트워크에 따라 다르게 적용되는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【청구항 12】

제 9항에 있어서, 상기 전송된 초기 네트워크간 연결요청 메세지를 분석하여 상기 제1 네트워크에 대한 시큐리티 레벨을 설정하는 단계는,

초기 네트워크간 연결요청 메세지를 분석하여 네트워크 연결허용 여부를 결정하는 단계를 포함하는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【청구항 13】

제 9항에 있어서, 상기 검색된 시큐리티 레벨 및 전송된 네트워크 명령 메세지를 제2 네트워크에 전송하는 단계는,

상기 제1 네트워크에 통지 메세지를 전송하는 단계를 포함하는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【청구항 14】

제 9항에 있어서,

상기 제2 네트워크가 상기 전송된 네트워크 명령 메세지에 대한 응답 메세지를 전송하는 단계; 및

상기 제2 네트워크의 응답 메세지에 대한 시큐리티 레벨을 체크하는 단계를 더 포함하는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【청구항 15】

제 9항에 있어서, 상기 전송된 네트워크 명령 메세지가 제2 네트워크 내 디바이스에 대한 서치 메세지인 경우,

상기 검색된 제1 네트워크의 시큐리티 레벨에 해당하는 디바이스들을 검색하여 전송하는 단계를 포함하는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【청구항 16】

제 9항에 있어서, 상기 전송된 네트워크 명령 메세지가 제2 네트워크 내 특정 디바이스를 요청하는 메세지인 경우,

상기 제2 네트워크에 저장되어 있는 디바이스의 서비스 컴포넌트 정보들 중 해당 디바이스의 컴포넌트 정보를 검색하여 전송하는 단계를 포함하는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【청구항 17】

제 9항에 있어서,

상기 제1 네트워크로부터 일정 시간 동안 네트워크 명령 메세지가 수신되지 않으면 상호 연결된 네트워크의 연결을 해지하는 단계를 더 포함하는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【청구항 18】

외부 네트워크로부터 초기 네트워크간 연결요청 메세지를 수신하는 단계;

상기 수신된 초기 네트워크간 연결요청 메세지를 분석하여 상기 외부 네트워크에 대한 시큐리티 레벨을 설정하는 단계;

상기 외부 네트워크로부터 네트워크 명령 메세지를 수신하는 단계;

상기 네트워크 명령 메세지를 전송한 외부 네트워크의 상기 설정된 시큐리티 레벨을 검색하는 단계; 및

상기 검색된 시큐리티 레벨 및 전송된 네트워크 명령 메세지를 자신의 네트워크로 전송하는 단계를 포함하는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【청구항 19】

제 18항에 있어서, 상기 네트워크간 연결요청 메세지는,

상기 네트워크간 연결요청 메세지를 보낸 외부 네트워크에 대한 정보를 포함하는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【청구항 20】

제 18항에 있어서, 상기 시큐리티 레벨은,

상기 연결되는 외부 네트워크에 따라 다르게 적용되는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【청구항 21】

제 18항에 있어서, 상기 수신된 초기 네트워크간 연결요청 메세지를 분석하여 상기 외부 네트워크에 대한 시큐리티 레벨을 설정하는 단계는,

초기 네트워크간 연결요청 메세지를 분석하여 네트워크 연결허용 여부를 결정하는 단계를 포함하는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【청구항 22】

제 18항에 있어서, 상기 검색된 시큐리티 레벨 및 전송된 네트워크 명령 메세지를 자신의 네트워크로 전송하는 단계는,

상기 외부 네트워크에 통지 메세지를 전송하는 단계를 포함하는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【청구항 23】

제 18항에 있어서,

상기 전송된 네트워크 명령 메세지에 대한 응답 메세지를 외부 네트워크로 전송하는 단계; 및

상기 전송하는 응답 메세지에 대한 시큐리티 레벨을 체크하는 단계를 더 포함하는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【청구항 24】

제 18항에 있어서, 상기 전송된 네트워크 명령 메세지가 네트워크 상의 디바이스에 대한 서치 메세지인 경우,

상기 검색된 외부 네트워크의 시큐리티 레벨에 해당하는 디바이스들을 검색하여 전송하는 단계를 포함하는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【청구항 25】

제 18항에 있어서, 상기 전송된 네트워크 명령 메세지가 네트워크 상의 특정 디바이스를 요청하는 메세지인 경우,

상기 요청된 특정 디바이스에 해당되는 디바이스의 서비스 컴포넌트 정보를 검색하여 전송하는 단계를 포함하는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

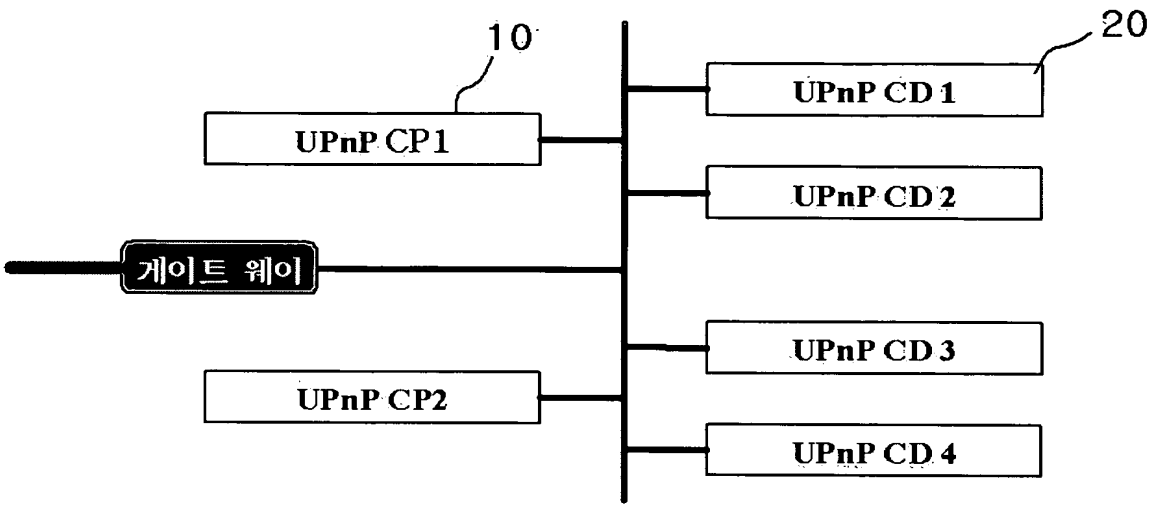
【청구항 26】

제 18항에 있어서,

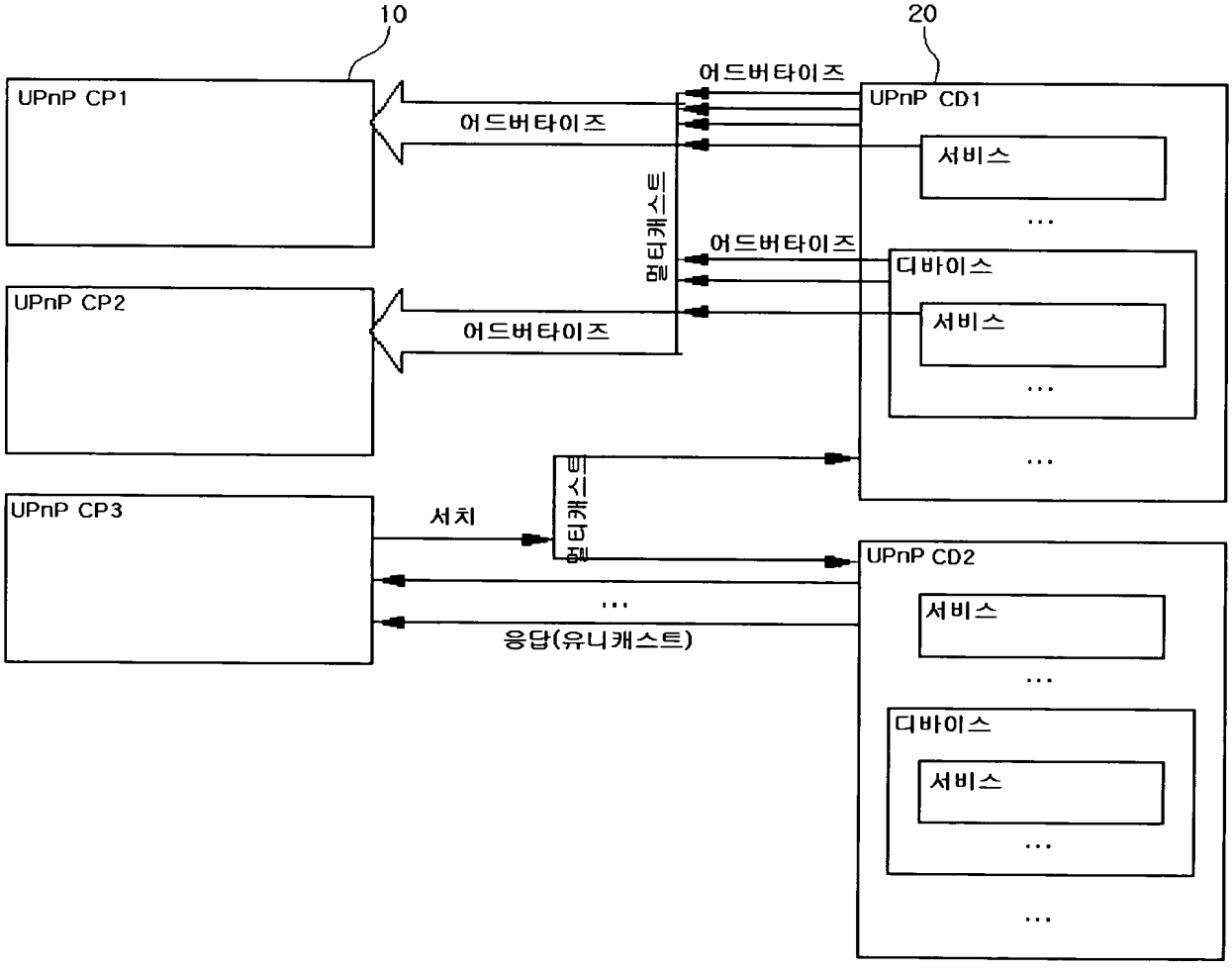
상기 외부 네트워크로부터 일정 시간 동안 네트워크 명령 메세지가 수신되지 않으면 상호 연결된 네트워크의 연결을 해지하는 단계를 더 포함하는 것을 특징으로 하는 개별적으로 존재하는 네트워크를 연결하는 방법.

【도면】

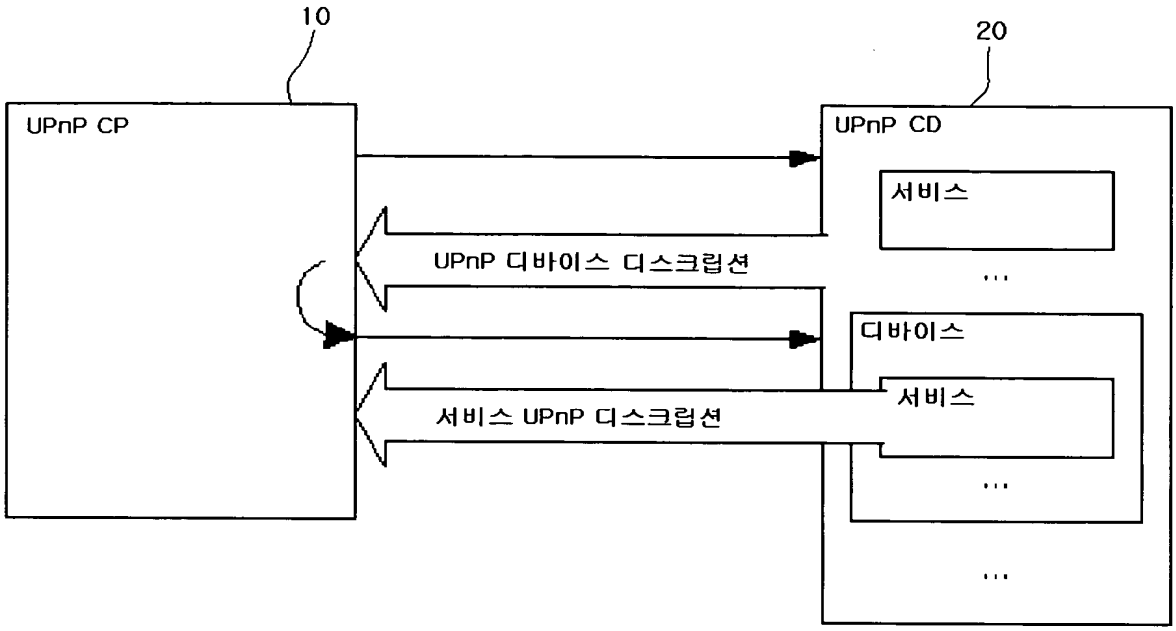
【도 1】


10
20
UPnP CP1
UPnP CD 1
UPnP CD 2
게이트 웨이
UPnP CD 3
UPnP CP2
UPnP CD 4

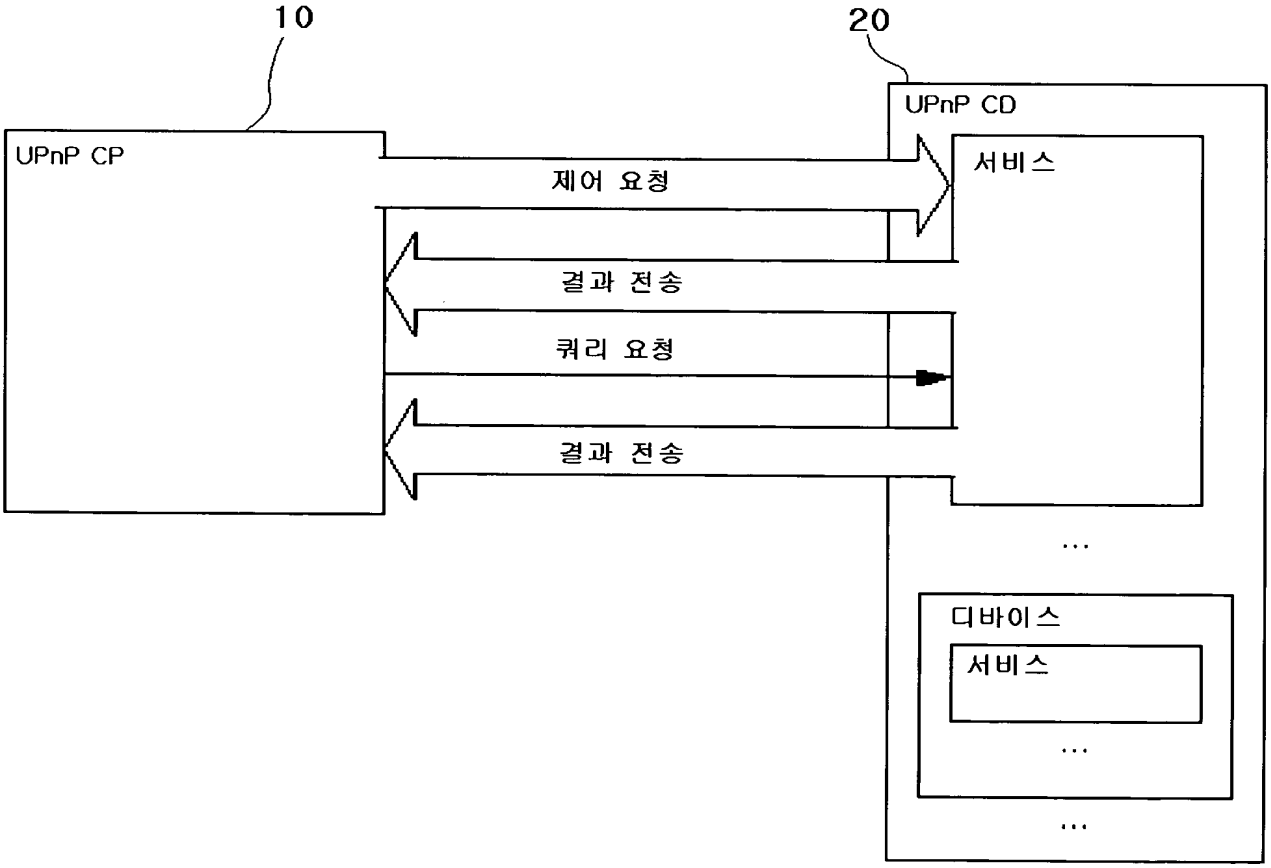
【도 2a】


10
20
UPnP CP1
어드버타이즈
UPnP CD1
어드버타이즈
서비스
...
멀티캐스트
어드버타이즈
디바이스
UPnP CP2
어드버타이즈
서비스
...
...
UPnP CP3
서치
멀티캐스트
UPnP CD2
...
서비스
응답(유니캐스트)
...
디바이스
서비스
...
...

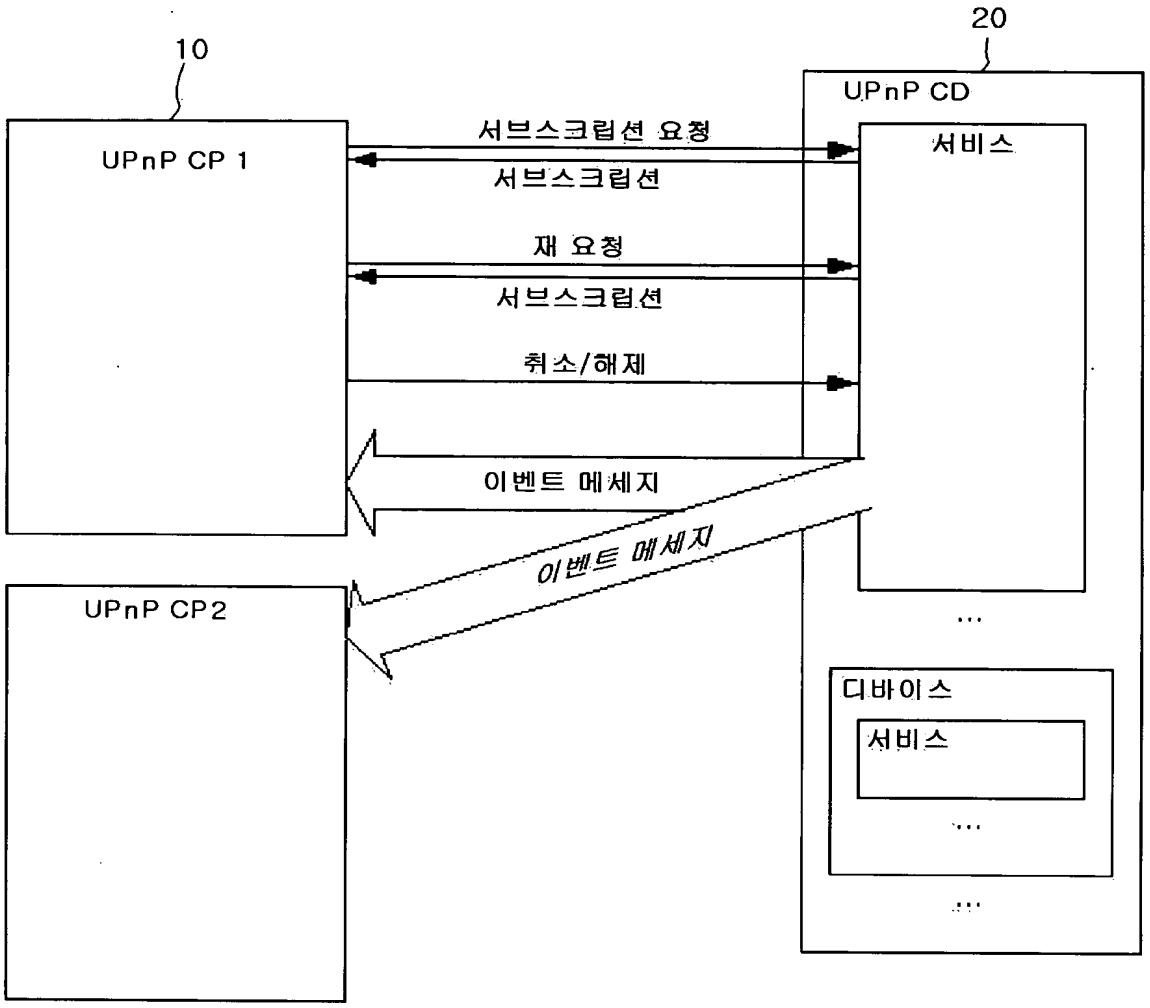
【도 2b】


10
20
UPnP CP
UPnP CD
서비스
...
UPnP 디바이스 디스크립션
디바이스
서비스
서비스 UPnP 디스크립션
...
...

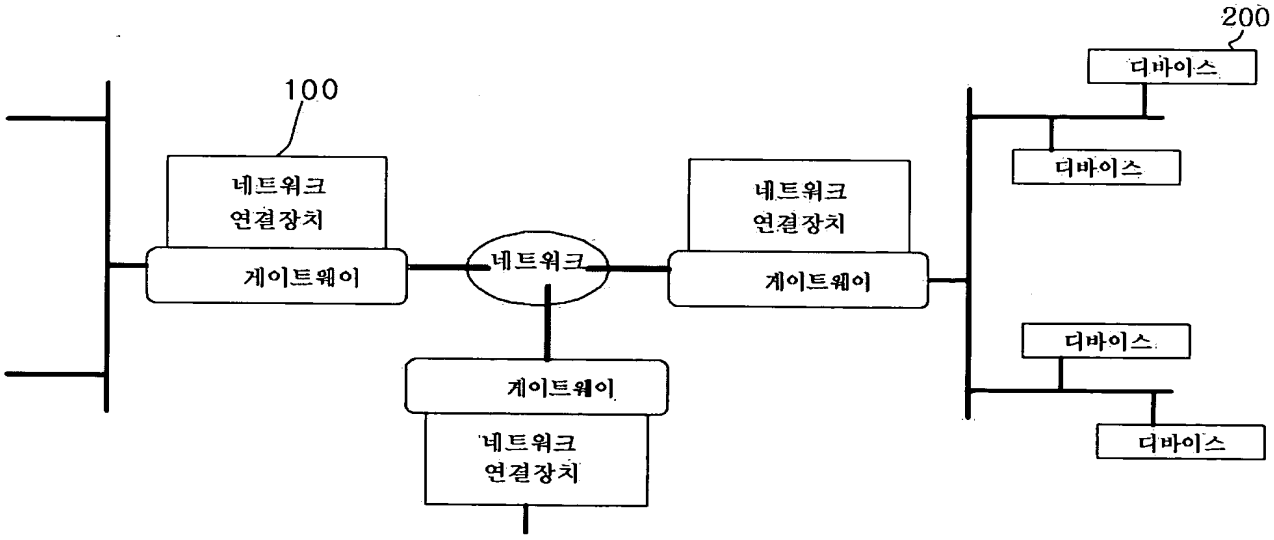
【도 2c】


10
20
UPnP CD
UPnP CP
서비스
제어 요청
결과 전송
쿼리 요청
결과 전송
...
디바이스
서비스
...
...

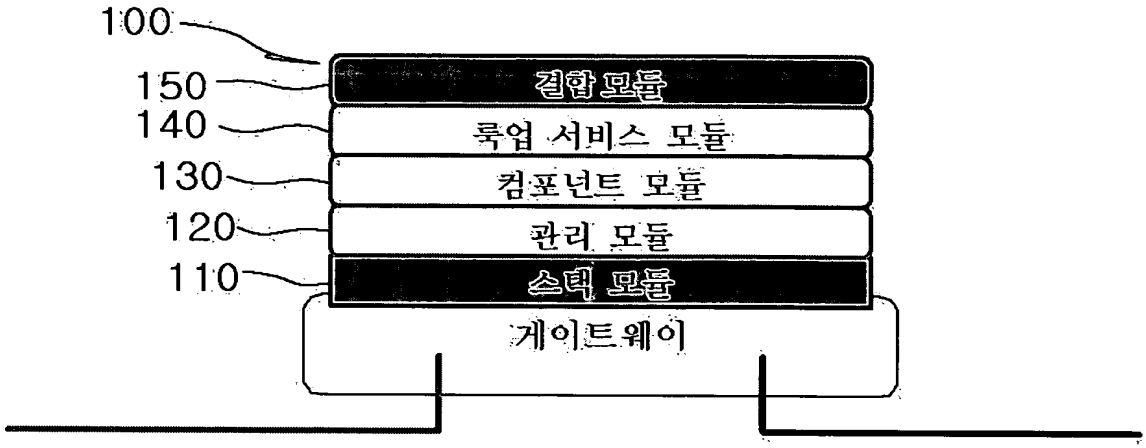
【도 2d】


10
20
UPnP CD
UPnP CP 1
서브스크립션 요청
서비스
서브스크립션
재 요청
서브스크립션
취소/해제
이벤트 메세지
이벤트 메세지
UPnP CP2
...
디바이스
서비스
...
...

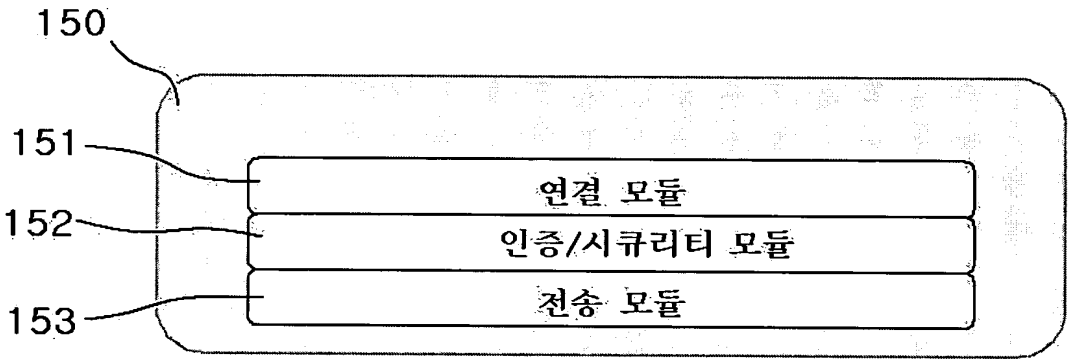
【도 3】


200
디바이스
100
네트워크 연결장치
게이트웨이
네트워크
네트워크 연결장치
게이트웨이
디바이스
디바이스
게이트웨이
네트워크 연결장치
디바이스

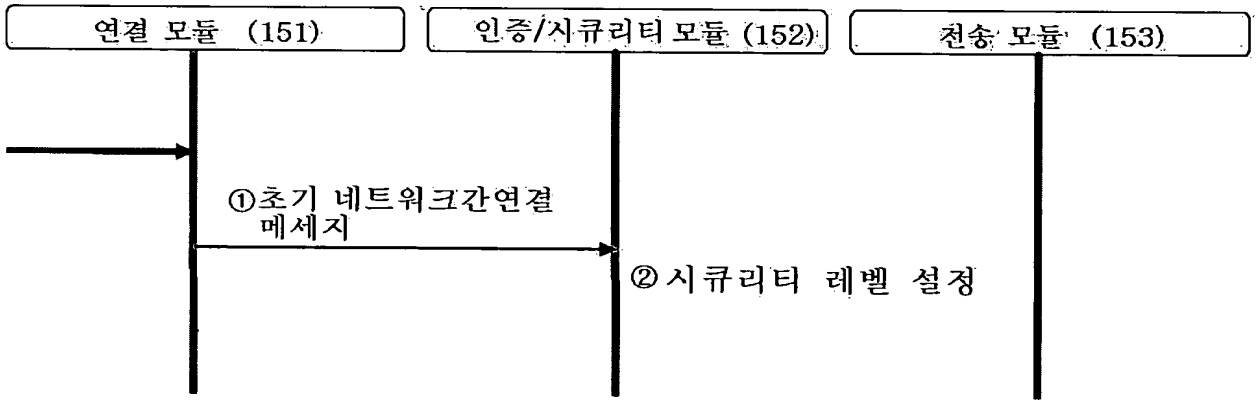
【도 4】


100
150
결합 모듈
140
룩업 서비스 모듈
130
컴포넌트 모듈
120
관리 모듈
110
스택 모듈
게이트웨이

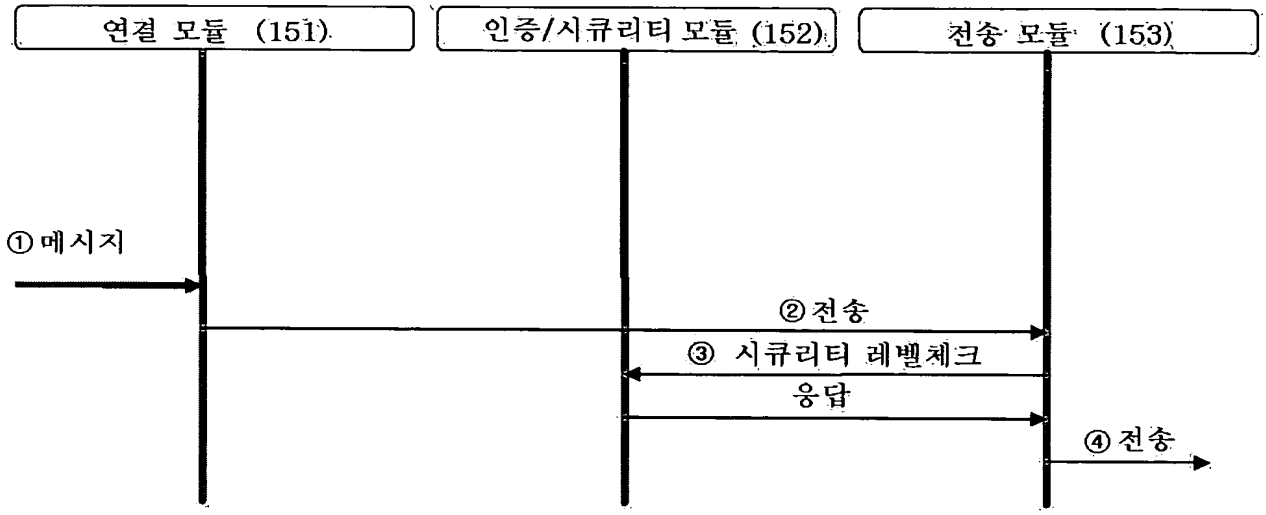
【도 5】


150
151
연결 모듈
152
인증/시큐리티 모듈
153
전송 모듈

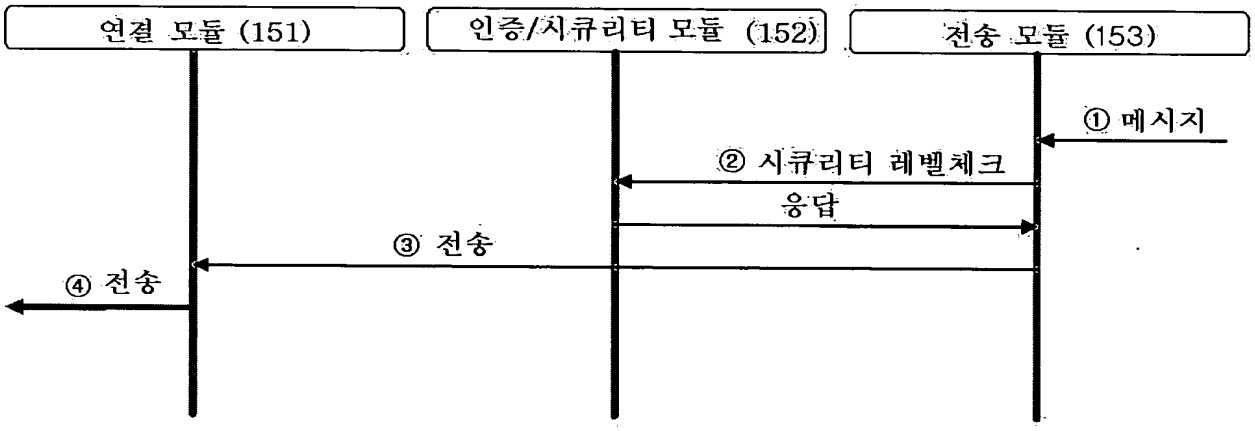
【도 6a】


연결 모듈 (151)
인증/시큐리티 모듈 (152)
전송 모듈 (153)
①초기 네트워크간연결 메세지
②시큐리티 레벨 설정

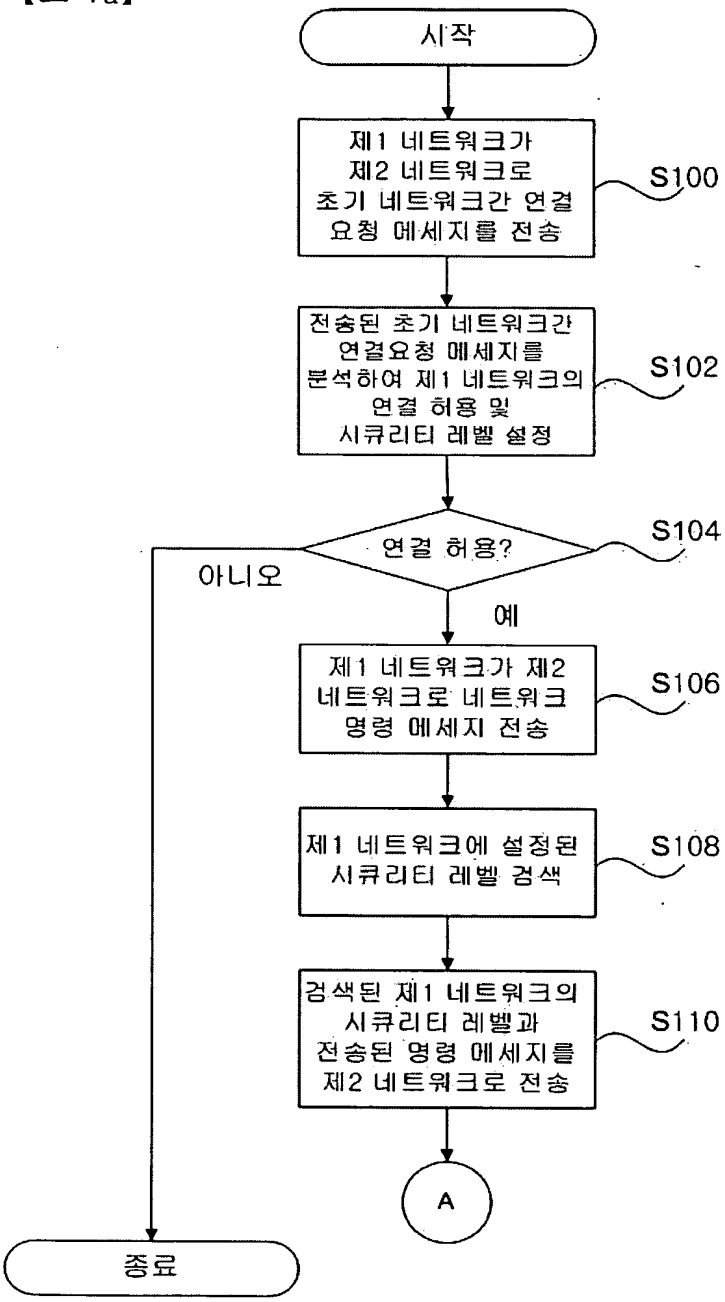
【도 6b】


연결 모듈 (151)
인증/시큐리티 모듈 (152)
전송 모듈 (153)
① 메시지
② 전송
③ 시큐리티 레벨체크
응답
④ 전송

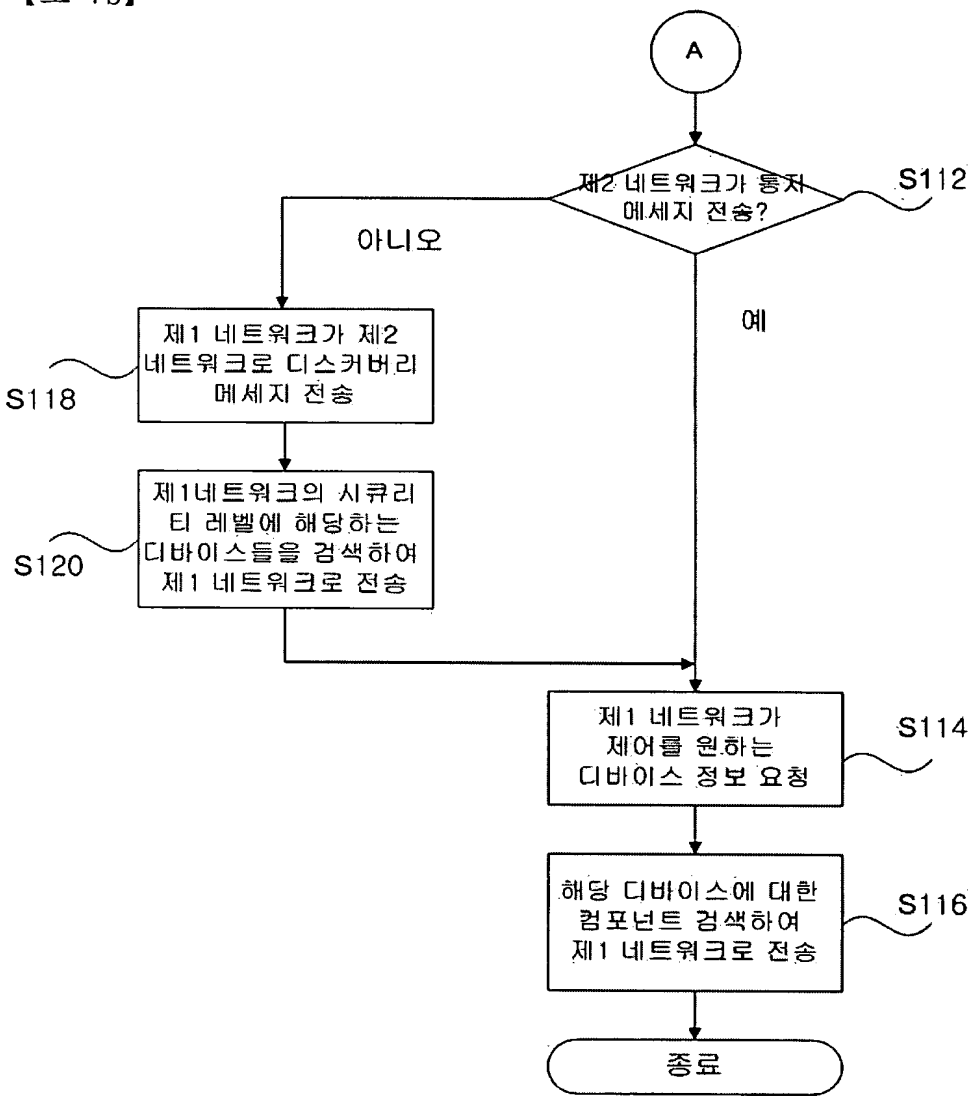
【도 6c】


연결 모듈 (151)
인증/시큐리티 모듈 (152)
전송 모듈 (153)
① 메시지
② 시큐리티 레벨체크
응답
③ 전송
④ 전송

【도 7a】


시작
제1 네트워크가 제2 네트워크로 초기 네트워크간 연결 요청 메세지를 전송
S100
전송된 초기 네트워크간 연결요청 메세지를 분석하여 제1 네트워크의 연결 허용 및 시큐리티 레벨 설정
S102
연결 허용?
S104
아니오
예
제1 네트워크가 제2 네트워크로 네트워크 명령 메세지 전송
S106
제1 네트워크에 설정된 시큐리티 레벨 검색
S108
검색된 제1 네트워크의 시큐리티 레벨과 전송된 명령 메세지를 제2 네트워크로 전송
S110
A
종료

【도 7b】


A
제2 네트워크가 통지 메세지 전송?
S112
아니오
예
제1 네트워크가 제2 네트워크로 디스커버리 메세지 전송
S118
제1네트워크의 시큐리티 레벨에 해당하는 디바이스들을 검색하여 제1 네트워크로 전송
S120
제1 네트워크가 제어를 원하는 디바이스 정보 요청
S114
해당 디바이스에 대한 컴포넌트 검색하여 제1 네트워크로 전송
S116
종료